RTU studiju kurss "Ievads kiberdrošībā"

33000 Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte

Vispārējā informācija

Kods	DE0834
Nosaukums	Ievads kiberdrošībā
Studiju kursa statuss programmā	Obligātais/Ierobežotās izvēles
Atbildīgais mācībspēks	Andrejs Romānovs - Doktors, Asociētais profesors
Mācībspēks	Heinrihs Kristians Skrodelis - Zinātniskais asistents Jūlija Strebko - Zinātniskais asistents
Apjoms daļās un kredītpunktos	1 daļa, 6.0 kredītpunkti
Studiju kursa īstenošanas valodas	LV, EN
Anotācija	Studiju kurss “Ievads kiberdrošībā” ir svarīga IT speciālista teorētiskās sagatavošanas sastāvdaļa, kas nodrošina studentam iespēju efektīvi orientēties mūsdienās IT un drošības problēmās. Kurss koncentrējas uz pamatiem un metodēm, kas nodrošina globālu pieeju uzņēmuma IT drošības organizācijai un vadības lēmumu pieņemšanai, lai nodrošinātu drošu un efektīvu uzņēmuma biznesa mērķu sasniegšanu. Kursā tiek izpētīta mūsdienīgā kiberdrošības pieeja kopējā uzņēmuma IT pārvaldības kontekstā, IT pārvaldības ietvari, uzņēmuma IT drošības stratēģija, IT pārvaldības kontroles metodoloģija un IT audits, kā arī veikta iegūto zināšanu praktiska pielietošana.
Mērķis un uzdevumi, izteikti kompetencēs un prasmēs	Sniegt padziļinātas zināšanas par jaunākajiem sasniegumiem kiberdrošības jomā. Iegūt zināšanas un praktiskās iemaņas kiberdrošības pieeju izmantošanā. Veicināt studenta spējas un kompetences izvēlieties kiberdrošības un IT pārvaldības ietvarus, metodoloģijas un standartus, definēt to izmantošanu uzņēmējdarbībā, piedāvājot alternatīvus risinājumus.
Patstāvīgais darbs, tā organizācija un uzdevumi	Studentu patstāvīgais darbs izpaužas šādās aktivitātēs: analītiskais darbs ar zinātnisko literatūru un citiem informācijas avotiem par kiberdrošības aktualitātēm un pieejām strādājot pie individuālā pētnieciskā projekta, prezentācijas sagatavošana par patstāvīgā pētījuma rezultātiem.
Literatūra	1. Obligātā. / Obligatory: 2. Don Franke. Cyber Security Basics: Protect your organization by applying the fundamentals. CreateSpace Independent Publishing Platform, 2016. 101 pp. 3. John Uwaya. Fundamental Cyber, Computing and Telephone Security. CreateSpace Independent Publishing Platform, 2018. 104 pp. 4. Steven De Haes, Wim Van Grembergen. Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer: Management for Professionals, 2016. 167 pp. 5. Randy A. Steinberg. Measuring ITSM: Measuring, Reporting, and Modeling the IT Service Management Metrics. Trafford, 2013. 196 pp. 6. Papildu. / Additional: 7. Tarantino Anthony. Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB's A-123, ASX 10, OECD Principles, Turnbull Guidance. Best Practices and Case Studies. Wiley, 2006, 336 pp.
Nepieciešamās priekšzināšanas	Pamatzināšanas informācijas tehnoloģijā.

Studiju kursa saturs

Saturs	Pilna un nepilna laika klātienes studijas		Nepilna laika neklātienes studijas	
	Kontakt stundas	Patstāv. darbs	Kontakt stundas	Patstāv. darbs
Mūsdienu kiberdrošības tendences un tehnoloģiskie pamati, veiksmes principi.	2	0	0	0
Kiberdrošības pārvaldība: komponenti, satvari un metodoloģijas, labākas prakses, sertifikācijas programmas.	4	4	0	0
Kopējais kiberdrošības BoK: informācijas drošības pārvaldība, lietojumprogrammu drošība, datortīklu drošība, mākoņdrošība, IoT drošība, drošā kodēšana, biometriskā drošība, kriptogrāfija, drošības arhitektūra, IT audits.	4	4	0	0
Kiberdrošības risku vadība: jēdziens, draudi, ievainojamības, riska novērtēšanas pieejas, drošības operāciju centri, reaģēšana uz incidentiem un digitālā kriminālistika.	2	6	0	0
Operāciju drošība OPSEC: pamatprincipi, operāciju drošības procesa kontrole, uzņemējdarbības nepārtrauktība un atkopšana.	2	4	0	0
Fiziskā drošība: draudi, administratīvā un tehniskā kontrole, piekļuves kontrole, fiziskās drošības kontrole, vides/dzīvības drošības kontrole.	2	6	0	0
Individuāls pētniecības projekts par galvenajām kiberdrošības tēmām: pikšķerēšana, ļaunprātīgas programmatūras analīze, drošā kodēšana, ievainojamības, kriptogrāfija, lietojumprogrammu drošība, tīkla drošība, mākoņa drošība, operētājsistēmu drošība, reaģēšana uz incidentiem, digitālā kriminālistika, kritiskās infrastruktūras drošība, lietu interneta drošība, blokķēdes drošība, biometrijas drošība, malu drošības pakalpojumi.	48	72	0	0
Kopā:	64	96	0	0

Sasniedzamie studiju rezultāti un to vērtēšana

Sasniedzamie studiju rezultāti	Rezultātu vērtēšanas metodes
Spēj definēt, interpretēt un lietot profesionālu terminoloģiju kiberdrošības jomā.	Zinātnisko diskusiju laikā ir parādītas spējas, izmantojot profesionālu terminoloģiju, raksturot problēmu un piedāvāt atbilstošu risinājumu.
Spēj argumentēti diskutēt par kiberdrošības risinājumu izvēli uzņēmuma problēmu risināšanā, tai skaitā prot apkopot kolēģu idejas strādājot grupās, un prezentēt grupas darba rezultātus.	Semināru un laboratorijas darbu laikā, balstoties uz teorētiskajām zināšanām un izmantojot profesionālu terminoloģiju, ir parādītas spējas konstruktīvi diskutēt par risināmo problēmu (izmantojot prāta vētras, diskusijas, problēmu risināšanu grupās u.c.).
Spēj analizēt konkrētas situācijas un izdarīt patstāvīgus secinājumus par kiberdrošības un IT pārvaldības metodoloģiju izmantošanu uzņēmuma darbībā.	Individuālā pētnieciskā projekta izstādes gaitā ir parādītas spējas piedāvāt alternatīvus risinājumus izvēlētajai problēmai, ka arī veikt šo alternatīvu salīdzinošu analīzi.
Spēj izskaidrot kiberdrošības pieeju pielietojuma būtību, iespējas un nozīmi uzņēmējdarbībā.	Eksāmena laikā ir demonstrēta spēja atpazīt formulētā uzdevuma būtību, kā arī lakoniski un argumentēti piedāvāt atbilstošu kiberdrošības risinājumu uzņēmējdarbības uzdevumiem.

Studiju rezultātu vērtēšanas kritēriji

Kritērijs	% no kopējā vērtējuma
Darbs semināros, diskusijās	20
Pētnieciskā projekta izstrāde	40
Eksāmens	40
Kopā:	100

Studiju kursa plānojums

Daļa	KP	Stundas			Pārbaudījumi		
		Lekcijas	Prakt d.	Laborat	Ieskaite	Eksām.	Darbs
1.	6.0	16.0	48.0	0.0		*	